REPLACEMENT SPECIFICATION

CLAIMS AND ABSTRACT

METHOD AND APPARATUS FOR CONTROLLING DIGITAL DATA

FIELD OF THE INVENTION

5

This invention relates to a technique for embedding additional information (digital watermark) into digital contents for copyright protection thereof, whereby a video recorder, a player or the like may detect such

10 embedded additional information for use in control (management) of recording and playback of such digital contents. More specifically, this invention relates to a method and an apparatus which use the digital watermarking and scrambling (or encrypting) techniques,

15 for controlling recording and playback of such digital contents.

BACKGROUND OF THE INVENTION

20 As one of the methods of providing the safest and powerful control function for copyright protection of digital data, there is the access control method of data that uses the so-called digital watermarking. Digital watermarking is a technique for electronically embedding

25 additional information into digital data (contents). Such additional information is embedded through a transformation of data itself.

That is, digital data and additional information are

30 unified or integrated together and, thus, it is difficult to separate the one from the other. In this respect, Japanese Patent Application 8-273551 discloses a prior technique for performing access control of data using this digital watermarking. More particularly, in

35 Japanese Patent Application 8-273551, an additional information detector (digital watermark detector) is provided in a drive such as DVD for detecting such additional information from various MPEG (Motion Picture Experts Group) streams and for performing access control

40 using the same.

Fig. 1 shows its schematic configuration. An STB (Set-Top Box) 110 supplies signals, which may be in analog or digital form, to a video recorder 120. In the

5 case of feeding an MPEG stream from the STB 11, this MPEG stream is directly sent to the additional information detector in the video recorder 120. On the other hand, if an output of the STB 110 is in analog form, this analog output is sent to an MPEG encoder in a video

10 driver card for converting it into a digital signal, which is then sent to the additional information detector.

This additional information detector detects any
15 additional information and copy mark information embedded in the contents and, in accordance with the information, performs a variety of predetermined controls with respect to the video recorder 120 and a playback machine (player) 130. By way of example, the following items of control
20 are performed.

In a recording device, detection of a digital watermark is performed and, based on this, the following copying control operations are performed (note that a
25 symbol "CM" below stands for a copy mark):
(1,0) and absence of CM: Add a CM and passes the stream (authorize or permit video recording).
(1,0) and presence of CM: Stop the stream or video recording.
30 (1,1)   : Stop the stream or video recording.
(0,0) or absence of detected additional information: Permit video recording.

35 In a playback device, detection of a digital watermark is performed and, based on this, the following playback control operations are performed:
(1,0) and absence of CM: Prohibit playback.
(1,0) and presence of CM: Prohibit playback for a
40 read-only disk, whereas permit playback for a write-once disk or a writeable disk.
(1,1)   : Permit playback for a read-only disk, whereas prohibit playback for a write-once disk or a writeable disk.
45 (0,0) or absence of detected additional information: Permit playback.

As described, Japanese Patent Application 8-273551

provides some copying control techniques, as well as
playback control techniques adapted for respective types
of media. However, in accordance with this prior
approach, it is necessary to provide the additional
5   information detector in a drive (i.e., in a recording
device or a playback device). This is because, in order
to secure copyright protection, it is mandatory to
provide the additional information detector at the
reading nucleus of the video recorder 120, even though
10   the video recorder 120 has severe constraints on its cost
and/or space.

Also, it is necessary to detect a digital watermark
from a variety of MPEG streams, which should inevitably
15   lead to upsizing of the detector. Further, in order to
know in the playback machine 130 that the current
contents is a copied one, it is necessary to know
information about types of the media (e.g., read-only,
write-once and writeable) that are subject to reading.
20   Accordingly, what is needed is a new copyright protection
scheme using digital watermarking, which is free of the
aforesaid problems.

SUMMARY OF THE INVENTION

25
It is, therefore, an object of this invention to
provide a method of controlling data copying or playback
and an apparatus therefor, which do not require provision
of an additional information detector in a drive that has
30   severe constraints on its cost and/or space.

It is another object of this invention to provide a
method of controlling data copying or playback and an
apparatus therefor, which use an additional information
35   detector of a smaller size.

It is yet another object of this invention to
provide a method of controlling data copying or playback
and an apparatus therefor, which do not require knowledge
40   of information about types of media for playback control.

It is yet another object of this invention to
provide a method of controlling data copying or playback
and a system therefor, which use effectively combined
45   digital watermarking and scrambling techniques.

To accomplish said objects, the recording control is performed as set forth below. First, from digital data, any additional information electronically embedded therein is detected and, if such additional information

5   is detected, then access control of the digital data is performed using the additional information. Next, the digital data is scrambled for recording the same onto a medium.

10   Note that the term "electronically embedded additional information" means herein such additional information that is embedded through a transformation of the data itself. Also, the term "access control" means herein to determine whether copying/recording of the

15   digital data is to be stopped or continued. Depending on a content of the additional information, the term "access control" also embraces embedding of control information such as a copy mark into the digital data.

20   Next, in case of playback control, the scrambled digital data is descrambled (or decrypted), thereby to detect any electronically embedded additional information and copy mark from the descrambled digital data. Using such detected information, playback control of the

25   digital data is performed.

The present invention relates to a method of recording digital data onto a medium starting with detection from digital data of any additional information

30   electronically embedded therein. If this additional information is detected, then access control is performed for the digital data using this additional information followed by scrambling the digital data and recording the scrambled digital data onto a medium.

35

The method can include the step of determining whether copying/recording of the digital data is to be stopped or continued and can further include a step of embedding a copy mark into the digital data in accordance

40   with a content of the aforesaid additional information.

Playback control of digital data recorded onto a medium is performed by descrambling the scrambled digital data, detecting from the digital data any additional

45   information and copy mark electronically embedded therein and performing playback control of the digital data using the additional information and copy mark. The electronically embedded additional information can

comprise such additional information that is embedded through a transformation of the data itself.

The present invention further contemplates a video driver card for creating digital data which card includes an encoder for receiving analog data and outputting digital data along with detection of any additional information electronically embedded in the digital data. The card can include structure for adding a copy mark to the aforesaid additional information in accordance with that additional information; and an arrangement for scrambling the digital data with the additional information. Where the digital data is an MPEG stream, the video driver card encoder is an MPEG encoder.

A video driver card of this invention for decoding digital data includes an arrangement for descrambling scrambled digital data along with an arrangement for detecting from the digital data any additional information and copy mark electronically embedded therein. The driver card can include the capability of performing playback control of the digital data using the additional information and copy mark. Where the digital data is an MPEG stream, the driver card includes means for determining whether or not outputting of an MPEG stream is to be performed and for outputting a desired MPEG stream.

The video driver card can further include means for adding a copy mark to the digital data in accordance with the additional information and copy mark and for outputting the digital data.

A recorder for recording digital data onto a medium in accordance with this invention employs an encoder for receiving analog data and outputting digital data along with a means for detecting any additional information electronically embedded in that digital data. This recorder is likewise capable of adding a copy mark to the aforesaid additional information in accordance with the additional information The recorder is further capable of scrambling the digital data and for recording the scrambled digital data onto a medium.

For digital data that is an MPEG stream, the encoder is an MPEG encoder. The electronically embedded additional information can comprise additional information that is embedded through a transformation of

the data itself.

Another aspect of this invention is a player for playing back digital data recorded onto a medium. It is capable of reading and descrambling the digital data from the medium. It can detect from the digital data any additional information and copy mark electronically embedded therein and can perform playback control of the digital data using the additional information and copy mark. Where the digital data is an MPEG stream, the player can determine whether or not outputting of an MPEG stream is to be performed and for outputting a desired MPEG stream.

The electronically embedded additional information can comprise such additional information that is embedded through a transformation of the data itself. The player can also include the ability to add a copy mark to the digital data in accordance with the additional information and copy mark and for outputting the digital data.

The foregoing and other features, utilities and advantages of the invention will be apparent from the following more particular description of a preferred embodiment of the invention as illustrated in the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWING

Fig. 1 is a diagram showing a prior scheme for performing access control of data.

Fig. 2 is a schematic diagram showing an apparatus of this invention for performing recording and playback of digital data.

Fig. 3 is another schematic diagram showing an apparatus of this invention for performing recording and playback of digital data.

Fig. 4 is a diagram showing paths of a signal, which is subject to prohibition of processing, and a medium in the prior scheme.

Fig. 5 is a diagram showing paths of a signal, which is subject to prohibition of processing, and a medium in accordance with the scheme of this invention.

5 Fig. 6 is an exemplary flow chart for recording/copying control.

Fig. 7 is an exemplary flow chart for playback control.

10 Fig. 8 is a block diagram showing a more detailed configuration of the apparatus for digital watermarking and scrambling.

Fig. 9 is a block diagram showing a more detailed
15 configuration of the apparatus for descrambling and detection of additional information.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

20 Fig. 6 shows an exemplary flow chart for recording/copying control. At step 610, digital data such as an MPEG stream is inputted, and at step 620, detection of any electronically embedded additional information is performed. At step 630, it is détermined
25 whether or not the additional information is detected, and if not, the stream is passed as it is.

If the determination at step 630 is "YES", then at step 640, it is determined whether or not the additional
30 information is (1,1), and if so, the stream is not passed. At the same time, scrambling or video recording is stopped. If the additional information is not (1,1), then at step 650, it is determined whether or not the additional information is (1,0).
35
If this result is "YES", the stream is passed as it is. If the result of step 650 is "NO", then at step 660, it is determined whether or not the additional information is (0,0). If this result is "YES", then the
40 stream is passed as it is. Otherwise, this means that the additional information is (0,1), which cannot possibly exist in any event and, thus, the additional information is determined to be undefined. Instead of doing this, however, the stream may be prohibited on an
45 assumption that such abnormality has been caused by an

erroneous bit change in the medium or another abnormality that occurred during embedding.

5   The passed stream is subsequently scrambled for recording the same onto a medium. While said scrambling is a means for enciphering, it may be such scrambling based on an encryption key for improving robustness. Using such scrambling by an encryption key, there is no way to decode the scrambled digital data in the absence 10   of the key and, thus, it becomes possible to distribute the digital contents in a safer manner.

    Fig. 7 shows an exemplary flow chart for playback control. At step 710, digital data is inputted, and at 15   step 720, descrambling (decoding) of the scrambled digital data is performed. At step 730, it is determined whether or not the decoding is terminated, and if so, the process proceeds to step 740.

20   If the result at step 730 is "NO", then at step 760, it is determined whether or not another encryption technique such as CSS (Content Scramble System) has been applied. Note here that CSS is a scrambling technique for a read-only disk. If the result at step 760 is 25   "YES", the corresponding decoding process is performed. Otherwise, the present playback is continued.

    After performing detection of the additional information at step 740, then at step 750, it is 30   determined whether or not the detection is terminated. If this result is "NO", the process proceeds to step 760. On the other hand, if the result of step 750 is "YES", the process proceeds to step 765.

35   At step 765, it is determined whether the detected additional information is (1,1) or (0,0) or absence of the additional information. If this result is "YES", the playback is continued. On the other hand, if this result is "NO", then at step 770, it is determined whether or 40   not the additional information is (1,0). If this result is "NO", the additional information is deemed to be undefined. However, if this result is "YES", then the process proceeds to step 780. At step 780, it is determined whether or not there exists a copy mark, and 45   if so, the playback is continued. On the other hand, if this result is "NO", then at step 790, a copy mark is added and the playback is continued. In this case, i.e., if the result of step 780 is "NO", the playback may be

alternatively stopped.

Incidentally, in a case where the digital data cannot be correctly descrambled (i.e., the digital data has not been scrambled), it may be alternatively processed as set forth below. For example, if the additional information is (1,0) and there is no copy mark, the stream is stopped and its descrambling or playback is stopped. Also, if the additional information is (1,1) and there is a copy mark, the stream is stopped and its descrambling or playback is stopped. Further, if the additional information is (1,1), the stream is descrambled and/or playback is stopped. Finally, if the additional information is (1,1) or there is no additional information at all, the playback is permitted.

Figs. 2 and 3 show schematic configurations of apparatuses of this invention for performing recording/playback of the digital data. While Fig. 2 shows an application of this invention to a video driver card primarily used in a personal computer in such a manner that a card is separated from a drive, Fig. 3 shows another application of this invention to a digital recorder (recorder) and a digital player (player) as representative electric home appliances in such a manner that a card and a drive are integrated together.

In Fig. 2, there are two different signal flows involved. That is, in the first signal flow, a signal inputted into an STB 210 is fed from an analog output of the STB 210 to a video driver card of a recorder 220. In the second signal flow, detection of additional information, addition of a copy mark and scrambling are performed in STB 210 and, then, the scrambled digital data is directly fed to a drive of the recorder 220.

When an analog signal is inputted to the video driver card, it is converted to digital data by an MPEG encoder such that detection of additional information, addition of a copy mark and scrambling are subsequently performed. The digital data so scrambled is recorded onto a medium by the recorder 220. This medium is then conveyed to a player 230 for its playback. Note that the recorder 220 and player 230 are described herein to be separate machines, but they may be configured as a single machine. The latter approach would be more general than the former.

The medium conveyed to the player 230 is subject to a reading operation. The digital data read from the medium is then inputted to a video driver card such that its descrambling, detection of the additional information

5   and addition of a copy mark (if required) are subsequently performed. Finally, the digital data is decoded by an MPEG decoder.

In Fig. 3, there are two different signal flows

10   involved. That is, in the first signal flow, a signal inputted into an STB 310 is fed from an analog output of the STB 310 to a recorder 320. Whereas in the second signal flow, detection of additional information, addition of a copy mark and scrambling are performed in

15   STB 310 and, then, the scrambled digital data is directly fed to a drive of the recorder 320.

When an analog signal is inputted to the recorder 320, it is converted to a digital data by an MPEG encoder

20   such that detection of additional information, addition of a copy mark and scrambling are subsequently performed. The digital data so scrambled is recorded onto a medium by a recording device. This medium is then conveyed to a player 330 for its playback. Note that the recorder 320

25   and player 330 are described herein to be separate machines, but they may be configured as a single machine. The latter approach would be more general than the former.

30   The medium conveyed to the player 330 is subject to a reading operation. The digital data read from the medium is then inputted to a video driver card such that its descrambling, detection of the additional information and addition of a copy mark (if required) are

35   subsequently performed. Finally, the digital data is decoded by an MPEG decoder.

Fig. 8 is a block diagram, which shows a more detailed configuration of the recorder 320 or STB adapted

40   for use in digital watermarking and scrambling. Block 810 is an input control circuit block for receiving an MPEG stream and passing the MPEG stream to a stream conversion circuit and an MPEG parser circuit. Block 820 is the MPEG parser circuit block for extracting from the

45   MPEG stream those portions that are required by the next stage. Block 830 is a macro block buffer for storing at least one macro block that is necessary for embedding control information.

Block 840 is a code amount comparison circuit block
for calculating and comparing code lengths in a macro
block. Block 850 is a code conversion circuit block for
5   converting a code to be used for embedding the control
information. Block 860 is a code amount adjustment
circuit block for adjusting a code length to be identical
to its value before the conversion and for forming the
result as an embedding conversion table.
10

Block 870 is a stream conversion circuit block for
stopping/converting/ passing the MPEG stream as it is
based on a detected result of additional information.
Block 880 is an accumulation memory for accumulating
15   those values of DCT factors derived by the MPEG parser
circuit that are multiplied by weighting factors. Block
890 is a table of the weighting factors for correlating
with additional information contained in the inputted
MPEG image.
20
Block 892 is a statistical processing circuit block
for performing statistical processing of the values
stored in the accumulation memory. Block 897 is a
detected result determination circuit block for
25   determining a value of embedded additional information
from its preceding stage and for issuing an indication to
the stream conversion circuit. Block 896 is a scramble
circuit block for performing authentication with a
recording device and for scrambling such stream that is
30   found to contain the additional information.

Fig. 9 is a block diagram, which shows a more
detailed configuration of the player 330 adapted for use
in descrambling and detection of the additional
35   information. Block 910 is a descramble circuit block for
authenticating an inputted digital signal with a playing
device and for descrambling the digital signal. Block
920 is an input control circuit block for receiving the
MPEG stream and passing the MPEG stream to a stream
40   control circuit and an MPEG parser circuit.

Block 930 is the MPEG parser circuit block for
extracting from the MPEG stream those portions that are
required by the next stage. Block 940 is an accumulation
45   memory for accumulating those values of DCT factors
derived by the MPEG parser circuit that are multiplied by
weighting factors. Block 950 is a table of the weighting
factors for correlating with additional information

contained in the inputted MPEG image.

Block 960 is a statistical processing circuit block
for performing statistical processing of the values
5   stored in the accumulation memory. Block 970 is a
detected result determination circuit block for
determining a value of embedded additional information
from its preceding stage and for issuing an indication to
the stream control circuit. Block 980 is the stream
10   control circuit for stopping/passing the MPEG stream as
it is based on the detected result of additional
information.

Fig. 4 shows paths of a signal, which is subject to
15   prohibition of processing, and a medium in the prior
scheme in case of only one generation copy is allowed.
In a compliant device (a device in accordance with the
prior scheme), a compliant source (a source in accordance
with the prior scheme) 410 is smoothly processed in a
20   recorder 420 and/or player 430, but no further recording
can be performed in recorder 440. Note, however, in this
respect that in such an operation combined with a non-
compliant device, it is possible to perform an illegal
recording/playback operation.
25

By way of example, if the compliant source 410 is
digitally inputted to a recorder 450 in the non-compliant
device, it is not only possible to perform its digital
recording but also its playback in a player 460.
30   Further, if a digital output of the player 430 in the
compliant device is inputted to a recorder 470 in the
non-compliant device, it becomes possible to perform its
recording as well.

35   Fig. 5 shows paths of a signal, which is subject to
prohibition of processing, and a medium in accordance
with the scheme of this invention. In a compliant device
(a device in accordance with the scheme of this
invention), a compliant source (a source in accordance
40   with the scheme of this invention) 510 is smoothly
processed in a recorder 520 and/or player 530, but no
further recording can be performed in a recorder 540.

Here, operations combined with a non-compliance
45   device will be considered briefly. First, even if it is
intended to digitally input the compliant source 510 to a
recorder 550 in the non-compliant device, such inputting
is prohibited and, thus, there will be no way to perform

its digital recording. Also, it becomes possible to prohibit inputting of a digital output of the player 530 in the compliant device to a recorder 570 in the non-compliant device.

5

Further, as another embodiment of playback control, for those scrambled contents of a read-only disk such as CSS, its playback may be permitted on a condition that CSS is successfully descrambled. More particularly, if
10 CSS is successfully descrambled, it is possible to avoid detection of any digital watermark.

Alternatively, if CSS is successfully descrambled, it is possible to permit playback on a condition that the
15 additional information of (1,1) is detected. Further, by adding a scheme that allows performance of descrambling using proximately detected digital watermarking information and/or additional information as a key, or to perform subsequent descrambling using such digital
20 watermarking information that is detected after the initial descrambling, it is possible to strengthen the protection function of scrambling and yet to cause detection of a digital watermark to be mandatory.

25 In order to protect copying of scrambled digital data, by using such scrambling with an encryption key, it becomes possible to disable its playback even though its copying is done. Moreover, for those contents that are not subject to any copyright protection, it is also
30 possible to avoid scrambling and/or embedding additional information therein, and to similarly apply descrambling in such a manner that any information to be displayed within a display unit such as a TV set is scrambled or additional information is detected, without departing the
35 spirit of this invention.

In accordance with this invention, there is provided a method of controlling data copying or playback and an apparatus therefor, which use effectively combined
40 digital watermarking and scrambling techniques. As a result, there is no need to provide an additional information detector in a drive that has severe constraints on its cost and/or space. Further, it becomes possible to prevent a compliant source from being
45 digitally recorded and/or digitally played back at a recorder and/or a player in a non-compliant device respectively.

While the invention has been particularly shown and described with reference to an exemplary preferred embodiment thereof, it will be understood by those skilled in the art that various other changes in the form and details may be made without departing from the spirit and scope of the invention.

What is claimed is: